# ASPI 6

# AVALIAÇÃO DA SEGURANÇA DA INFORMAÇÃO EM SISTEMAS CONTÁBEIS

A segurança da informação em sistemas contábeis nunca esteve tão em alta nos últimos anos. Com o advento da tecnologia e seu progresso ao decorrer dos anos, é inegável que houve e há muitos benefícios oriundos desse constante desenvolvimento tecnológico. Porém, a contrapartida desse desenvolvimento, são os riscos e vulnerabilidade das informações das organizações que são colocadas em xeque.

Com a evolução da tecnologia, todas as áreas começaram a aderir e se amoldar à tecnologia. Na área da contábil não foi diferente, os escritórios que, outrora, eram arcaicos e com processos manuais demandando tempo e esforço, hoje, entretanto, trabalham com sistemas otimizados que substituem serviços braçais e manuais que, épocas atrás, eram de extrema relevância.

Ao trabalhar e se apropriar da tecnologia, os escritórios perceberam os inúmeros benefícios que esta trouxe, tanto relativo à informação quanto a dinamicidade entre os processos contábeis.

À medida que as organizações contábeis foram se apropriando dessa tecnologia, foi aumentando a preocupação com a segurança e a confiabilidade dessas informações transitadas dentro do sistema contábil.

Os administradores e gestores começaram a perceber que a transição de informação estava ficando cada vez mais vulnerável, pois a transição dessas informações transcorria pelos colaboradores contábeis. Embora os sistemas hoje em dia sejam otimizados, ainda assim, há a necessidade do colaborador alimentar o sistema manualmente, seja com informação ou na geração de relatórios.

Contudo, nenhuma solução ou mecanismo tecnológico é suficiente para garantir a eficiência e eficácia do sistema de segurança da informação contábil. Pode-se afirmar, portanto, que os sistemas de informações contábeis são limitados com relação a segurança da informação, embora traga incontáveis benefícios para as organizações.

A segurança da informação, nos dias de hoje, é tratada como uma forma de gestão de negócios, protegendo as informações, diminuindo os riscos e ameaças contra a confiabilidade e autenticidade dessas informações. A gestão de segurança da informação tem por objetivo evitar vazamentos, fraudes, espionagem comercial, sabotagem e diversos outros riscos e problemas que possam prejudicar as pessoas e as empresas.

Sabendo disso, os órgãos responsáveis por regular a profissão contábil no Brasil, em dezembro de 2011, emitiu um CPC – Comitê de Pronunciamento Contábeis – aprovando uma nova estrutura, citando pressupostos básicos relevantes para a profissão, além de citar três atributos necessários para a confiabilidade da informação contábil, que são: completude, neutralidade e exatidão.


A completude da informação passa por questões ligadas à realidade econômica, onde há toda informação necessária para que o usuário da informação compreenda o fenômeno retratado.

A neutralidade se relaciona à capacidade de retratar a realidade econômica desprovida de algum viés, tanto na seleção quanto na apresentação da informação contábil-financeira. Por fim, a exatidão perpassa pela representação fidedigna, ou seja, a isenção de erros, além de evitar omissões de fenômenos retratados para os usuários da informação. É, portanto, necessário todo esse aparato para que a informação financeira e contábil seja relevante para a tomada de decisões, mesmo que, contudo, os usuários não desejem aproveitá-las.

A segurança das informações contábeis não é apenas incumbência da contabilidade ou, até mesmo, do TI, mas, sim, uma responsabilidade atribuída à alta gerência. Portanto, a segurança das informações se tornou uma obrigação para a administração e gestores da empresa, de modo que mantenham controles internos onde garantem que as informações sejam precisas, oportunas e, principalmente, seguras.

O controle interno é um sistema dentro de um sistema, onde protege o negócio contra abusos e fraudes, garantindo que as informações que o sistema receba sejam oportunas e precisas e que todos os requisitos necessários estejam em conformidade.

Esses requisitos passam por cinco elementos-chave de controle interno:

- Controle ambiental;
- Avaliação de risco;
- Procedimento de controle;
- Monitoramento;
- Informação e comunicação;

O controle ambiental refere-se à atitude e ao comportamento da gerência e dos funcionários na empresa, onde as metas e os objetivos estipulados pela administração afetarão, diretamente, o comportamento dos funcionários, pois pode gerar inflexibilidade na busca por atingir a determinados níveis de vendas a todo custo. O departamento de recursos humanos tem papel fundamental nesse controle, pois fornecerá todo o suporte e contribuição para que haja controle ambiental efetivo.

A avaliação de risco incorpora a capacidade do negócio de analisar seus riscos, estimar sua importância e agir e reagir de acordo com elas. Além disso, é uma função gerencial, mas que pode ser delegada à funcionários.

Procedimentos de controle, simplesmente fornece métodos para executar os controles citados, de modo a diminuir a beneficiar tanto a empresa quanto o funcionário.

O monitoramento dos controles internos é tratado como o elemento de feedback do processo. É de extrema relevância o monitoramento, pois é a partir dele que o negócio consegue determinar a eficácia dos sistemas.

Por fim, o último elemento-chave é os procedimentos de informação e comunicação do negócio.

Para que o procedimento seja executado, em grande parte, depende das informações que é fornecida por cada departamento, de maneira que essas informações sejam oportunas e honestas, bem como precisas e úteis.

É indubitável que a segurança e integridade das informações contábeis hoje é um grande desafio para as organizações, porém a implementação de sistemas que forneçam garantias razoáveis, onde produzirá informações relevantes e confiáveis para atender às necessidades de relatórios internos e externos é vital para a vida e reputação da organização.

**Medidas de Segurança**

As medidas de segurança são conhecidas, também, como controles e podem ser preventivas, para evitar riscos, ou investigativas, onde visa identificar os problemas após os fatos ocorridos. Algumas medidas de segurança, por exemplo, são:

- Mudanças frequentes de senha;
- Criptografia de dados;
- Revisão mensal do supervisor de relatórios de fornecedores;
- Servidor seguro e proteção do ambiente computacional;
- Arquivamento off-site seguro e protegido de backup.


Controles de segurança referem-se a ferramentas que fornecem serviços de segurança, como, por exemplo, senhas e firewalls. O controle de segurança dos sistemas de informação é um meio de garantir a continuidade dos negócios e minimizar danos aos negócios, evitando e diminuindo o efeito de ameaças ao sistema.

A segurança da informação, portanto, deve ser utilizada com o objetivo principal de proteger os dados, resguardando a organização de riscos e perigos que possam expor os clientes e usuários das informações contábeis, além dos empresários que utilizam o sistema para realizar diversas atividades, principalmente, relatórios informativos sobre as empresas para as quais a contabilidade presta serviço.